



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/876,351	06/06/2001	Doug Joseph	BEA92001008US1	9150
49474	7590	06/12/2006	EXAMINER	
LAW OFFICES OF MICHAEL DRYJA 704 228TH AVE NE #694 SAMMAMISH, WA 98074			POLTORAK, PIOTR	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 06/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/876,351

Applicant(s)

JOSEPH ET AL.

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-8 and 10-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 3-8 and 10-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

The Amendment, and remarks therein, received on 4/4/06 have been entered and carefully considered.

Response to Amendment

1. Applicant arguments regarding the 35 USC § 112 first paragraph have been considered and found persuasive. In light of applicant's remarks the examiner agrees that one of ordinary skill in the art would be able to implement the invention as described by the claim language using hardware. The software is frequently utilized to accomplish computer tasks using computer hardware. The claim language does not prohibit the use of software and in fact explicitly suggests such an implementation (e.g. claim 15).

As a result in light of applicant's arguments and amendments to the claim language the 35 USC § 112 rejections cited in the previous Office Action are withdrawn.

2. As per the 35 USC § 103 rejections applicant's main argument addressing invalidity of rejection is that the art or record used in combination is not compatible and citing In re Ratti applicant suggests that "combination of references would require a substantial reconstruction and redesign of the elements". Applicant follows the assumption with the allegation that the use of Pfleeger in Stein's invention would require "complete redesign of the web browser- and indeed, the operating system on which the web browser runs, the operating system kernel, and the security kernel". The examiner respectfully points out that the statements are faulty.

Stein's disclosure that SSL transaction occurs between a client and a server wherein a "client can be a web browser or other end-user process" does not necessarily means that a web browser application has access to encryption keys. SSL is a security protocol layered beneath an application protocol used by an application program to communicate over a network (see the disclosure of SSL patent (U.S. Patent No. 5825890) for example).

Furthermore, even if someone introduced key exchange and encryption process to be handled by web browser application, separation of encryption functionalities from user processes would not require any radical reconstruction and redesigning of the web browser, the operating system on which the web browser runs, the operating system kernel, and the security kernel. To illustrate the examiner points to the one of the most common operating system incorporating web browsers: Windows.

Windows' security functions are handled by the Security Reference Monitor operating in the Kernel Mode in order to separate the security operation from user processes. (See Windows NT 4.0 operating system architecture (Hadfield, Fig. 3.4, pg. 76) for example).

However, upon closer investigation of Pfleeger's disclosure the examiner found that Pfleeger's suggestion to separate user processes from security functions is inconclusive as Pfleeger suggests that "some activities related to protection functions are performed outside the security kernel" (Pfleeger, pg. 302). As a result the 35 USC § 103 rejection presented in the previous Office Action is withdrawn.

3. However, the new search resulted in newly discovered prior art. The new rejection follows below.
4. Claims 1, 3-8 and 10-18 have been examined.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 11 and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

It is not clear whether the statement “the key is inaccessible by all user processes running on the ...” suggests that none of the user processes are able to access the key or whether the statement should be treated as though some user processes can access the key and some cannot, thus not all user process can access the key.

Below, the examiner illustrates two acceptable meaning of this limitation by addressing the independent claims limitations using two different types of rejections.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2134

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 3-7, 10-12, 15-16 are rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and further in view of Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00).
- As per claims 1, 3-4 and 7 Stein teaches SSL transaction between a client (browser) and a server, wherein a key, identification of the first node, and identification of the second node is sent from hardware of the first node (a node hosting the client browser) to hardware of the second node (the node hosting the server) (pg. 41, Fig. 3.2 transaction 6, and pg. 42 first §), receiving the key identification of the first node, and identification of the second node by the hardware of the second node and verifying the identification of the first node (pg. 41, Fig. 3.2, transaction 7, pg.42 second §) and the identification of the second node at the hardware of the second node , and storing the key at the hardware of the second node (pg. 42 first §). Once a SSL connection is in place the secure hardware of the first hardware and the secure hardware of the second node establish a channel over which the process of the first node and the process of the second node are able to communicate (SSL Characteristics, in particular pg. 40).

Stein does not explicitly teach that the second keys are inaccessible by all user processes.

Marino discloses keys inaccessible by all user processes (Fig. 2 and col. 3 lines 40-44). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent all user processes from accessing keys as taught by Marino. One of ordinary skill in the art would have been motivated to prevent all user processes from accessing keys in order to minimize opportunity for security violation.

Neither Stein nor Marino discloses that unauthorized processes running on the first node are unable to send unauthorized messages.

Fontana teaches unable unauthorized processes running on computer nodes to send unauthorized messages. In particular, Fontana teaches Microsoft Outlook E-mail security patch that prevents unauthorized processes from sending unauthorized messages (Fontana, pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages as taught by Fontana. One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent worms from spreading to other nodes.

7. Claims 11 and 15 are substantially equivalent to claim 1; therefore claims 11 and 15 are similarly rejected.

8. As per claim 5-6 and 10 SSL is implemented using TCP/IP, which is a protocol that includes source and destination ports and the SSL tunnel is established for the purpose of exchanging data, wherein the data is encrypted. As a result processing received messages after they are decrypted is implicit.
9. As per claims 12 and 16 Stein, Marino and Fontana do not explicitly teach a key table. However, storing a key for inter-node communication would have been implicit so that the entire session could be encrypted. Furthermore, Official Notice is taken that it is old and well-known practice to utilize table data structure to store data given benefit of a quick and easy data retrieval using tables.
10. Claims 1, 3-7, 10-12, 15-16 are rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and further in view of Carter (U.S. Patent No. 5845331).

As per claims 1, 3-4 and 7 Stein teaches SSL transaction between a client (browser) and a server, wherein a key, identification of the first node, and identification of the second node is sent from hardware of the first node (a node hosting the client browser) to hardware of the second node (the node hosting the server) (pg. 41, Fig. 3.2 transaction 6, and pg. 42 first §), receiving the key identification of the first node, and identification of the second node by the hardware of the second node and verifying the identification of the first node (pg. 41, Fig. 3.2, transaction 7, pg.42 second §) and the identification of the second node at the hardware of the second node , and storing the key at the hardware of the second node (pg. 42 first §). Once

a SSL connection is in place the secure hardware of the first hardware and the secure hardware of the second node establish a channel over which the process of the first node and the process of the second node are able to communicate (SSL Characteristics, in particular pg. 40).

Stein does not explicitly teach that the second keys are inaccessible by all user processes.

Marino discloses keys inaccessible by all user processes (Fig. 2 and col. 3 lines 40-44). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent all user processes from accessing keys as taught by Marino. One of ordinary skill in the art would have been motivated to prevent all user processes from accessing keys in order to minimize opportunity for security violation.

Neither Stein nor Marino discloses that unauthorized processes running on the first node are unable to send unauthorized messages.

Carter teaches to preventing unauthorized processes to conduct unauthorized activities (col. 1 lines 24-35), which reads on preventing unauthorized processes to unable to send unauthorized messages.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages. One of ordinary skill in the art would have been motivated to prevent unauthorized processes running on the first node to send unauthorized

messages in order to restrict secure sending messages to only authorized processes.

11. Claims 11 and 15 are substantially equivalent to claim 1; therefore claims 11 and 15 are similarly rejected.

12. As per claim 5-6 and 10 SSL is implemented using TCP/IP, which is a protocol that includes source and destination ports and the SSL tunnel is established for the purpose of exchanging data, wherein the data is encrypted. As a result processing received messages after they are decrypted is implicit.

13. As per claims 12 and 16 Stein, Marino and Carter do not explicitly teach a key table. However, storing a key for inter-node communication would have been implicit so that the entire session could be encrypted. Furthermore, Official Notice is taken that it is old and well-known practice to utilize table data structure to store data given benefit of a quick and easy data retrieval using tables.

14. Claim 8 is rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Security, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00) and further in view of Boden (U.S. Patent No. 6182228). Stein, Marino and Fontana do not teach verifying the identification of the first node and the identification of the second node.

Stein, Marino and Fontana do not explicitly teach that the verifying the identification of the first node and the second node by comprises verifying the identification of the

first node and the identification of the second node in a channel state table accessible by the hardware of the second node and inaccessible by all the user processes of the second node.

Boden teach verifying the identification of the first node and the identification of the second node in a channel state table (col. 3 lines 9-60).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to verify the identification of the first node and the identification of the second node in a channel state table as taught by Boden. One of ordinary skill in the art would have been motivated to perform such a modification in order to restrict the inter-node communication only to the particular nodes.

The information in the channel state table disclosed by Boden is sensitive information that with security violations could compromise the overall system. Thus, restricting user processes from accessing the channel state table in order to minimize any security violation as aimed by Marino's invention would be implicit.

15. Claim 8 is rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Security, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and Carter (U.S. Patent No. 5845331) and further in view of Boden (U.S. Patent No. 6182228).

Stein, Marino and Carter do not teach verifying the identification of the first node and the identification of the second node.

Stein, Marino and Carter do not explicitly teach that the verifying the identification of the first node and the second node by comprises verifying the identification of the

first node and the identification of the second node in a channel state table accessible by the hardware of the second node and inaccessible by all the user processes of the second node.

Boden teach verifying the identification of the first node and the identification of the second node in a channel state table (Boden, col. 3 lines 9-60).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to verify the identification of the first node and the identification of the second node in a channel state table as taught by Boden. One of ordinary skill in the art would have been motivated to perform such a modification in order to restrict the inter-node communication only to the particular nodes.

The information in the channel state table disclosed by Boden is sensitive information that with security violations could compromise the overall system. Thus, restricting user processes from accessing the channel state table in order to minimize any security violation as aimed by Marino's invention would be implicit.

16. Claims 13 and 17 are rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and further in view of Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00) and further in view of Benedyk et al. (U.S. Pub. No. 20010055380) and Bean (U.S. Patent No.4843541).

Stein, Marino and Fontana teach a system for inter-node communication as discussed above.

17. As per claims 13 and 17 Stein, Marino and Fontana do not explicitly teach connection tables accessible to secure connection management hardware mechanisms of communicating nodes, wherein the connection tables have number of entries, each entry identifying one of the user processes of both communicating inter-nodes.

18. Benedyk teach a connection table with a number of entries, each identifying one of the user processes of both communicating inter-node (Benedyk, Fig. 8).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate a connection table as taught by Benedyk. One of ordinary skill in the art would have been motivated to perform such a modification in order to allow easy communication in a TCP/IP based networks by providing easy access to access to fundamental information required in the TCP communication.

The examiner points out that although the explicit example of the claim limitations were provided, defining ports in TCP/IP communication is old and well known in the art of computing. In fact some of the ports used by the most common applications are referred to as "Well-known" ports.

19. Stein, Marino, Fontana and Benedyk do not explicitly teach that the connection table identifies one or more partitions of the particular node.

20. Bean teach unique partition identifiers identifying nodes partitions (Bean, col. 50 lines 55-66).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include partition identifiers as taught by Bean within the first and second connection tables given the benefit of the security enhancement and operation speed in systems hosting plurality of different preferred guest programming systems running simultaneously in the different partitions.

21. Claims 14 and 18 are rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Security, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and further in view of Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00) and further in view of Benedyk (U.S. Pub. No. 20010055380), Bean (U.S. Patent No.4843541) and Boden (U.S. Patent No. 6182228).
Stein, Marino and Fontana in view of Benedyk and Bean's invention has been discussed above.

22. Claim 14 and 18 introduces the limitations substantially equivalent to the limitations of claim 8; therefore these limitations are similarly rejected.

23. Claims 13 and 17 are rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and further in view of Carter (U.S. Patent No. 5845331) and further in view of Benedyk et al. (U.S. Pub. No. 20010055380) and Bean (U.S. Patent No.4843541).

Stein, Marino and Carter teach a system for inter-node communication as discussed above.

24. As per claims 13 and 17 Stein, Marino and Carter do not explicitly teach connection tables accessible to secure connection management hardware mechanisms of communicating nodes, wherein the connection tables have number of entries, each entry identifying one of the user processes of both communicating inter-nodes.

25. Benedyk teach a connection table with a number of entries, each identifying one of the user processes of both communicating inter-node (Benedyk et al., Fig. 8).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate a connection table as taught by Benedyk et al. One of ordinary skill in the art would have been motivated to perform such a modification in order to allow easy communication in a TCP/IP based networks by providing easy access to access to fundamental information required in the TCP communication.

The examiner points out that although the explicit example of the claim limitations were provided, defining ports in TCP/IP communication is old and well known in the art of computing. In fact some of the ports used by the most common applications are referred to as "Well-known" ports.

26. Stein, Marino, Carter and Benedyk do not explicitly teach that the connection table identifies one or more partitions of the particular node.

27. Bean et al. teach unique partition identifiers identifying nodes partitions (col. 50 lines 55-66).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include partition identifiers as taught by Bean et al. within the first and second connection tables given the benefit of the security enhancement and operation speed in systems hosting plurality of different preferred guest programming systems running simultaneously in the different partitions.

28. Claims 14 and 18 are rejected under 35 U.S.C. 103 (a) as being obvious over Stein (Lincoln D. Stein, "Web Security, a step-by -step reference guide", 1998, ISBN: 0201634899) in view of Marino (U.S. Patent 5530758) and further in view of Carter (U.S. Patent No. 5845331) and further in view of Benedyk (U.S. Pub. No. 20010055380), Bean (U.S. Patent No.4843541) and Boden (U.S. Patent No. 6182228).

Stein, Marino and Carter in view of Benedyk and Bean's invention has been discussed above.

29. Claim 14 and 18 introduces the limitations substantially equivalent to the limitations of claim 8; therefore these limitations are similarly rejected.

30. Claims 1, 3-7, 11 and 15 are rejected under 35 U.S.C. 103 (a) as being obvious over Windows NT as illustrated by winnt40serv and Microsoft Press in view of Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899) and further in view of Fontana (John Fontana, Defending against Outlook viruses, http://www.networkworld.com/archive/2000/99914_07-03-2000.html, 07/03/00).

As per claims 1, 3-4 and 7, as well known in the art Windows NT operating system is a product running on computer hardware devices that comprise a plurality of user processes. Some of the processes assist users with common activities: Notepad and Text Editor (winnt40serv, pg. 4), calculator and clock (winnt40serv, pg. 5), multimedia (winnt40serv, pg. 18-19) etc. and some provide network services: a browser (winnt40serv, pg. 10) and Internet Information Server (IIS, Microsoft Press, pg. 1 and 8, Minasi, pg. 1050-1052) for example. In addition IIS is able to provide SSL transactions (Microsoft Press, pg. 359) and Stein discloses SSL transaction as a secure transaction between a first node (browser) and a second node (server), wherein a key, identification of the first node, and identification of the second node is sent from hardware of the first node (a node hosting the client browser) to hardware of the second node (the node hosting the server) (Stein, pg. 41, Fig. 3.2 transaction 6, and pg. 42 first §), receiving the key identification of the first node, and identification of the second node by the hardware of the second node and verifying the identification of the first node (Stein, pg. 41, Fig. 3.2, transaction 7, pg.42 second §) and the identification of the second node at the hardware of the second node , and storing the key at the hardware of the second node (Stein, pg. 42 first §). Once a SSL connection is in place the secure hardware of the first hardware and the secure hardware of the second node establish a channel over which the process of the first node and the process of the second node are able to communicate (Stein, SSL Characteristics, in particular pg. 40).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure some of the user processes (e.g. a browser and IIS server) in two hardware nodes utilizing network communication such as Window NT to access keys as disclosed by *Stein* given the benefit of secure communication.

Of course, just as it would have been obvious to give access to keys to user processes utilized in communication (e.g. a browser) there is no need whatsoever to give the access to the keys used in communication to other processes such as a calculator or a notepad. Given access to the keys to only some processes result in the keys being inaccessible by all user processes running on the nodes.

Neither Windows NT nor *Stein* discloses that unauthorized processes running on the first node are unable to send unauthorized messages.

Fontana teaches unable unauthorized processes running on computer nodes to send unauthorized messages. In particular, Fontana teaches Microsoft Outlook E-mail security patch that prevents unauthorized processes from sending unauthorized messages (Fontana, pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages as taught by Fontana. One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent worms from spreading to other nodes.

31. Claims 11 and 15 are substantially equivalent to claim 1; therefore claims 11 and 15 are similarly rejected.

32. Claims 1, 3-7, 11 and 15 are rejected under 35 U.S.C. 103 (a) as being obvious over Windows NT as illustrated by winnt40serv and Microsoft Press in view of Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899) and further in view of view of Carter et al. (U.S. Patent No. 5845331). As per claims 1, 3-4 and 7, as well known in the art Windows NT operating system is a product running on computer hardware devices that comprise a plurality of user processes. Some of the processes assist users with common activities: Notepad and Text Editor (winnt40serv, pg. 4), calculator and clock (winnt40serv, pg. 5), multimedia (winnt40serv, pg. 18-19) etc. and some provide network services: a browser (winnt40serv, pg. 10) and Internet Information Server (IIS, Microsoft Press, pg. 1 and 8, Minasi, pg. 1050-1052) for example. In addition IIS is able to provide SSL transactions (Microsoft Press, pg. 359) and Stein discloses SSL transaction as a secure transaction between a first node (browser) and a second node (server), wherein a key, identification of the first node, and identification of the second node is sent from hardware of the first node (a node hosting the client browser) to hardware of the second node (the node hosting the server) (Stein, pg. 41, Fig. 3.2 transaction 6, and pg. 42 first §), receiving the key identification of the first node, and identification of the second node by the hardware of the second node and verifying the identification of the first node (Stein, pg. 41, Fig. 3.2, transaction 7, pg.42 second §) and the identification of the second node at the hardware of the second node , and storing the key at the hardware of the second node (Stein, pg. 42 first §). Once a SSL connection is in place the secure hardware of the first hardware and the

secure hardware of the second node establish a channel over which the process of the first node and the process of the second node are able to communicate (Stein, SSL Characteristics, in particular pg. 40).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure some of the user processes (e.g. a browser and IIS server) in two hardware nodes utilizing network communication such as Window NT to access keys as disclosed by *Stein* given the benefit of secure communication.

Of course, just as it would have been obvious to give access to keys to user processes utilized in communication (*e.g. a browser*) there is no need whatsoever to give the access to the keys used in communication to other processes such as a calculator or a notepad. Given access to the keys to only some processes result in the keys being inaccessible by all user processes running on the nodes.

Neither Windows NT nor Stein explicitly disclose that unauthorized processes running on the first node are unable to send unauthorized messages.

Carter teaches enabling unauthorized process running to send unauthorized messages. In particular, Carter et al. teach to preventing unauthorized processes to conduct unauthorized activities (col. 1 lines 24-35), which reads on preventing unauthorized processes to unable to send unauthorized messages.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to prevent unauthorized processes running on the first node to send unauthorized messages. One of ordinary skill in the art would have been motivated

to perform such a modification in order to secure sending messages to only authorized processes.


33. Claims 11 and 15 are substantially equivalent to claim 1; therefore claims 11 and 15 are similarly rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


6/1/06


JACQUES H. LOUIS JACQUES
PRIMARY EXAMINER